Virus Pengikut Aliran Brontok

Entah mengapa pesan dari virus ini mirip dengan Brontok. Anda pasti sudah kenal dengan Brontok, *kan*? Ya, Brontok merupakan salah satu virus yang "katanya" membawa pesan moral yang idealis. Sama halnya dengan virus yang akan kita bahas kali ini.

Arief Prabowo

Salah satu file virus yang menyamar sebagai folder.

Tak jelas kenapa alasannya. Apakah pembuat virus ini hanya ingin mengikuti jejak Brontok, atau ia merupakan salah satu anggota dari JowoBot Community yang ditengarai merupakan kelompok pembuat virus Brontok itu? Hanya ia yang tahu. Yang jelas, virus ini telah cukup banyak menyebar di masyarakat.

Tercatat Tim PC Media Antivirus sudah banyak mendapatkan laporan dari pembaca bahwa komputernya terserang oleh virus Babat ini. Dari beberapa contoh file yang didapat, virus ini memiliki tiga varian. Dan ini tidak menutup kemungkinan bahwa di luar sana masih terdapat varian lain dari virus Babat. PC Media Antivirus mengenali Babat sebagai Babat-B.A, Babat-B.B, dan Babat-C, atau pada antivirus lain ada yang mengenalnya sebagai virus Hadus atau Kiamat.

Teknologi yang dipakai virus yang dapat menyebar pada *operating system* berbasis Windows XP ini sebenarnya sudah sangat lazim dipergunakan oleh kebanyakan virus lokal sekarang, yakni icon yang menyerupai gambar folder standar bawaan Windows, dan diprogram menggunakan bahasa Visual Basic. Ketiga varian dari virus ini memiliki ukuran yang berbeda–beda, yakni 81.920 untuk Babat-B.A dan Babat-B.B, serta 49.152 bytes untuk Babat-C. Kesemuanya merupakan file executable murni, tidak di-*compress*.

PCMAV dapat mengatasi virus Babat.

Pada sistem yang terinfeksi oleh virus ini, di memory akan terdapat tiga process yang berjalan, yakni dengan nama ISASS.exe, kernel32.bat, dan LNETINFO.exe. Nama process yang digunakan memang dibuat sedemikian rupa agar mirip dengan *process* atau *service* milik Windows tentunya agar user terkecoh. Selain itu, ciri virus yang lainnya adalah pada *version information* yang terdapat pada virus ini, yakni apabila kita melakukan klik kanan file *Virus|Properties|Version*, maka pada Internal Name misalnya akan terdapat string "File Folder". Maksudnya agar lebih meyakinkan dengan icon berupa Folder dan version information juga berupa "File Folder".

Metode Infeksi

Pada saat file virus ini kali pertama dijalankan, ia akan menampilkan isi dari My Documents pada Windows Explorer. Padahal di balik itu, ia telah melakukan penginfeksian atas sistem tersebut. Ia akan membuat duplikat atas dirinya yang merupakan file induk pada beberapa tempat di komputer Anda, dan menyembunyikannya dengan memberikan *attribut hidden*. Beberapa file induk tersebut terletak pada \%SYSTEMDIR%\ISASS.exe, \%WINDIR%\security\kernel32.bat, \%SYSTEMDIR%\LNETINFO.exe, dan beberapa file duplikat lainnya yang akan memanggil file induk tersebut contohnya pada direktori "\Documents and Settings\All Users\Start Menu\Programs\Startup\Temp.pif". Setelah virus menetap di memory, ia akan membuat perubahan di registry agar virusnya dapat aktif pada saat memulai Windows.

Registry yang diinfeksi adalah pada key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ctfmon, HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Kiamat Sudah Dekat, dan HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell, atau pada varian lain ada juga yang menginfeksi key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\(Default) atau HKCU\Software\Microsoft\Windows\CurrentVersion\Run\msconfig. Inilah merupakan salah satu yang membedakan antarbeberapa variannya, yakni pada penamaan item saat infeksi di registry, penamaan file duplikat virus, dan penambahan daftar beberapa program yang di-*black list* oleh Babat.

Virus ini selanjutnya juga akan membuat salinan tubuhnya, contohnya "C:\Windows\System32.exe" dan menyembunyikan direktori "C:\Windows\System32\". Maksudnya untuk mengecoh user apabila ingin mengklik atau masuk ke direktori System32 padahal yang ia klik adalah virusnya sendiri.

Pada direktori My Documents, virus juga akan membuat duplikat dirinya dengan nama "Data %COMPUTERNAME%.exe". %COMPUTERNAME% di sini merupakan nama dari komputer tersebut. Lalu di dalam direktori My Music akan terdapat "My Music.exe" dan My Pictures juga akan terdapat "My Pictures.exe". Selain itu, di root direktori pada beberapa drive

akan terdapat file "%COMPUTERNAME% Punya.exe". Pada variant lain, pada direktori Desktop juga akan terdapat file dengan nama "My Documents.exe".

Stay Resident in Memory

Setelah virus bersemayam di memory, yang ia lakukan adalah memonitor setiap aksi yang dilakukan oleh *user*. Apabila virus mengetahui bahwa registry item yang dibuat oleh virus dihapus oleh sang user, maka dengan segera virus akan membuatnya lagi.

Dalam interval waktu tertentu, virus juga melakukan pengecekan terhadap process-nya sendiri. Apabila salah satu dari ketiga process virus tersebut tidak ada, ia akan menjalankan lagi process yang hilang tersebut. Dengan kata lain, ia akan memeriksa teman-temannya di memory, apabila salah satu tidak ada, ia akan memanggilnya kembali.

Babat juga akan melakukan penginfeksian pada drive di komputer dengan melakukan pencarian dibeberapa drive atau storage devices di komputer tersebut. Misalnya pada komputer Anda terdapat sebuah direktori "D:\Data-Data", maka di dalam direktori tersebut akan terdapat sebuah file virus dengan nama menyerupai nama direktori tempatnya berada, yakni menjadi "Data-Data.exe".

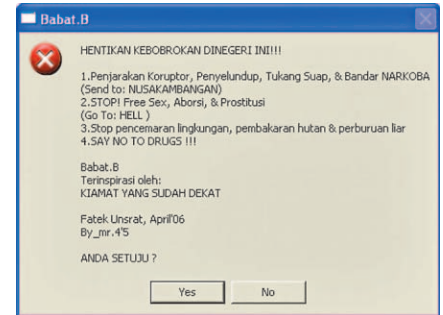
Walau virus ini tidak menghapus data dokumen kita, namun ia juga dapat menghapus file program. Misalnya lagi, apabila Anda memiliki sebuah program yang biasa dijalankan, contoh terletak pada "D:\WinAmp\WinAmp.exe", karena virus ini akan menginfeksi direktori dengan nama menyerupai nama direktori asli. Jadi, walaupun pada direktori tersebut sudah ditemukan file program asli dengan nama "WinAmp.exe", ia akan tetap menimpa (*overwrite*) program tersebut dengan tubuhnya sendiri.

Aksi Lainnya

Selain dapat menyebar melalui media penyimpan data misalnya Flash Disk, ia juga dapat menyebar melalui jaringan. Contohnya apabila direktori yang mengandung virus tersebut di share ke jaringan, orang lain yang mengakses file virus pada jaringan akan terinfeksi juga.

Satu hal penting yang dikatakan di awal, virus ini akan menampilkan pesan yang hampir mirip dengan Brontok dalam bentuk *Dialog Box*. Mekanismenya adalah pada interval waktu tertentu, file induk yang telah menetap di memory akan memanggil sebuah file virus yang sebelumnya telah ia letakkan pada \%SYSTEMDIR%\Kiamat.exe. File itulah yang akan menampilan pesan dari pembuatnya itu.

Sebenarnya file tersebut sama seperti tubuh virus Babat lainnya, tapi dalam hal ini yang membedakan adalah nama file dan tempat dari file tersebut berada. Apabila yang dijalankan "C:\Windows\System32\Kiamat.exe", maka tampilkan dialog box pesan, kalau bukan ia hanya akan menginfeksi sistem. Pada pesan yang ditampilkan juga terdapat dua tombol, yakni *Yes* dan *No*. Apabila tombol Yes ditekan, pesan tersebut akan menutup, tapi apabila tombol No yang ditekan, komputer akan *restart*.

Babat juga melakukan beberapa perubahan di registry yang tujuannya untuk menonaktifkan beberapa fitur penting dari Windows dan agar penyamarannya sebagai folder dapat lebih meyakinkan. Beberapa fitur Windows yang dinonaktifkan olehnya adalah fasilitas *Run, Task Manager, Folder Options, Regedit*, dan *Find*. Tak lupa ia juga menge-set agar Windows Explorer tidak menampilkan file atau folder dengan attribut hidden dan juga menyembunyikan extension file.

Tampilan pesan dari virus Babat.

Babat akan melakukan investigasi terhadap program–program yang dijalankan oleh user. Yakni, apabila menjalankan suatu program yang dianggapnya akan menggangu kelangsungan hidupnya, maka dengan segera Windows akan di-restart olehnya.

Beberapa program tersebut adalah msconfig.exe, regedit.exe, taskmgr.exe, cmd.exe , setup.exe, install.exe, dan rstrui.exe. Terlihat bahwa virus tersebut akan menghalangi user untuk menggunakan beberapa program bawaan Windows, menginstal suatu aplikasi, dan mengakses System Restore. Karena System Restore dapat digunakan untuk mengembalikan sistem kepada kondisi beberapa waktu lalu, misalnya pada saat komputer belum terinfeksi oleh virus ini. Sebenarnya penggunaan System Restore untuk menghapus virus ini juga tidak terlalu disarankan karena virus juga masih terdapat pada beberapa tempat di komputer Anda yang kemungkinan besar masih dapat aktif lagi. Walau daftar program yang di-*black list* tersebut tidak sebanyak Brontok, tapi daftar ini sepertinya terus ditambahkan pada varian–varian selanjutnya.

Babat juga melakukan *back-up* terhadap file MSVBVM60.DLL pada direktori \WINDOWS\security\ms.inf.

Pembasmian dan Pencegahan

PC Media Antivirus (PCMAV) sudah dapat mengenali dan membasmi virus ini dengan baik. Untuk membasminya, silakan scan seluruh drive dengan PC Media Antivirus RC9 ini. Untuk pencegahan, sebaiknya setiap melakukan transfer data entah itu dari Flash Disk ataupun data yang Anda *download*, hendaknya scan dahulu dengan Antivirus kesayangan Anda. Tapi, apabila ternyata PCMAV tidak dapat mengenali virus Babat yang jelas–jelas terdapat pada komputer Anda, dengan senang hati kami akan menerima contoh virus yang Anda kirimkan. Kami tunggu! ■

Menginfeksi folder dengan nama sama seperti nama folder-nya.